CHECK POINT™

CloudGuard
WAF

Preemptive Web Application & API Protection

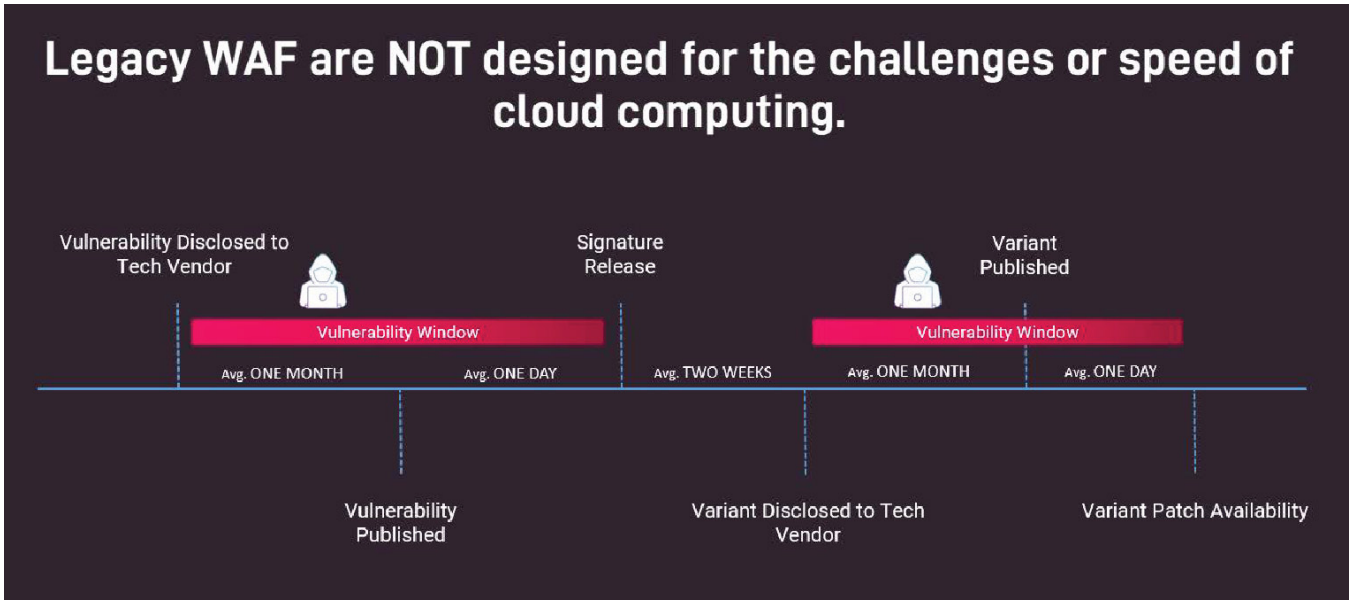
Don't Get Caught Off-Guard

As your cloud based web applications expand, so does your vulnerability to cyber threats. Attackers exploit your Web Applications and APIs using nefarious techniques like SQL injection, cross-site scripting and automated scripts a.k.a "bots." The fallout from such assaults can be highly detrimental and financially devastating, making application security an absolute priority for any business, big or small.

Traditional WAF Just Can't Cut It!

Web application firewalls (WAFs) have traditionally relied on threat signature mapping to reactively fend off attacks. This approach is both reactive (takes and avg of 1 month for initial rememdy) and is limited in its effectiveness because it can only make a binary decision: block or permit. This leads to a high number of false positives, causing headaches for security teams who must constantly monitor and maintain them.

With modern applications being developed and deployed at breakneck speed, it is becoming increasingly clear that this outdated approach is unable to keep up with the pace and scope of DevOps practices.



Eliminate Risks, Reduce Overheads, Accelerate Development

CloudGuard WAF is the ultimate solution for organizations looking to mitigate risks and speed up development. This advanced cloud native platform streamlines Application security management and re-imagines threat prevention, effectively blocking known and unknown threats and significantly reducing operational overheads.

Real-time Preemptive Protection

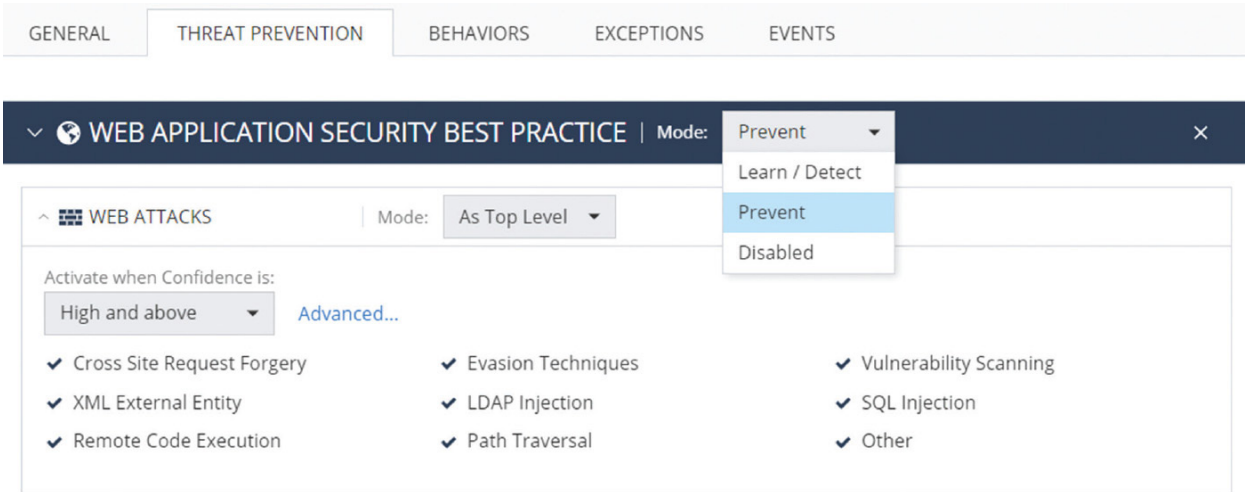
CloudGuard WAF preemptively blocks attacks, based on patented contextual AI/ML. WAF embeds security testing directly into the development pipeline, providing real-time protection. The result is enhanced security, accelerated time to-market, and greater development efficiency, all achieved without compromising on quality or safety.

Precise Prevention

CloudGuard WAF accurately eliminates false positives by examining various contextual parameters and determining a final risk score with input from multiple ML engines. Using multiple engine risk analysis provides more accurate decisionmaking eradicating manual tuning and enabling security admins to operate confidently in Prevent Mode without blocking legitimate requests.

Business Specific Protection

Web apps enter learning mode to gather environment-specific data and business cases, with multiple CPUs storing and synchronizing information hourly. Thesystem id entifies the source, HTTP method, HTTP requests, and every key/value pair, quickly completing its learning before users switch to prevent mode.

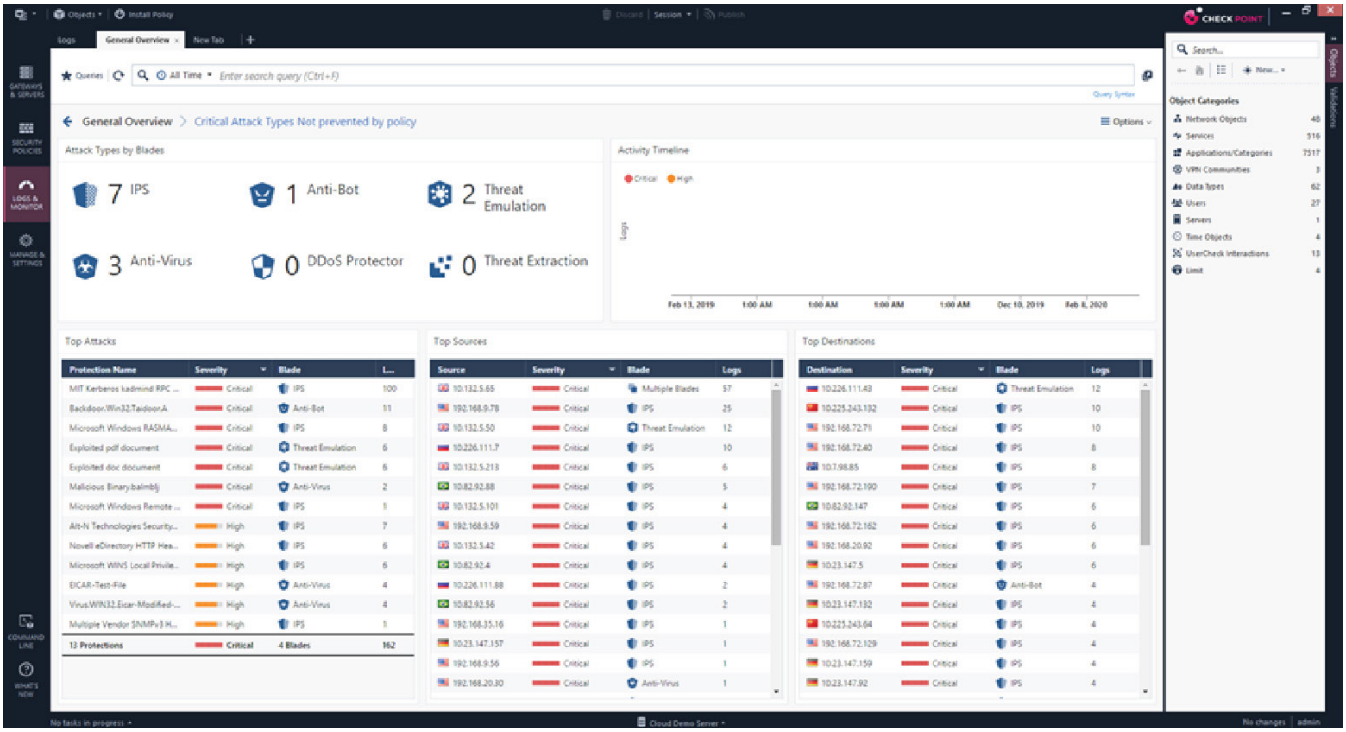


API Discovery

Applications are evolving faster than ever and as they do, they create and expose more APIs. Ensure that your application's APIs are being used correctly, with CloudGuard WAF's API discovery, as well as auto generated OpenAPI SWAGGER schema files. Stop cyber criminals from leveraging your APIs to expose sensitive data, inject commands or to extract API keys.

Prevent Automated Attacks

Protect your applications from sophisticated bots. CloudGuard uses JS injections to perform clientside behavioral analysis (including biometric activity like key strokes and mouse movements), in order to distinguish between human and non-human interactions with your application. Stop credential stuffing, brute force attacks and site scraping with advanced bot protection.



AUTOMATED WEB APPLICATION AND API PROTECTION (WAF)

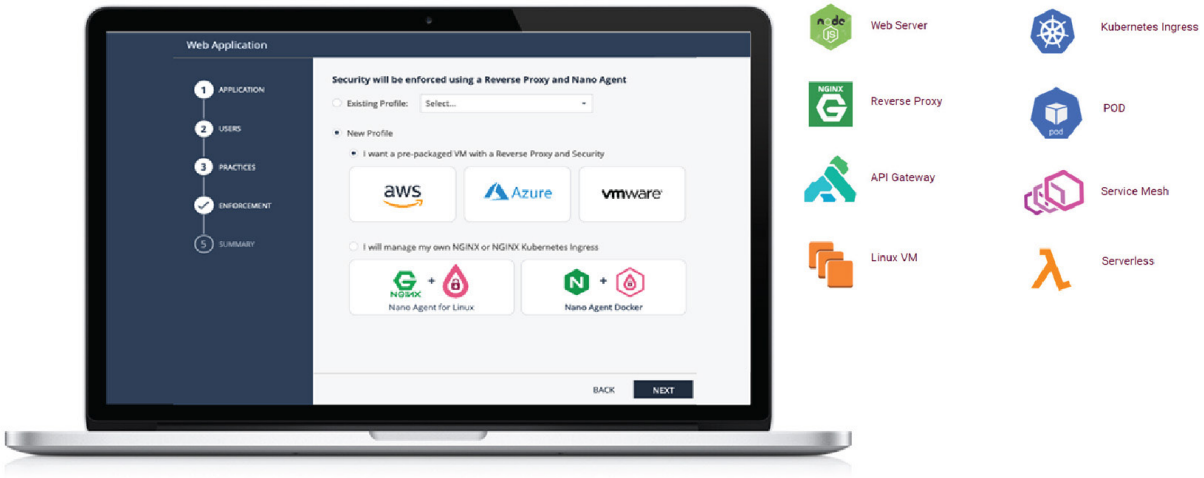
- Web Application Protection
- API Security
- Bot Prevention
- Intrusion Prevention (IPS)
- File Security

KEY PRODUCT BENEFITS

- **Preemptive Protection:** Contextual machine learning provides preciseanalysis, preventing known and unknown cyber attacks
- **CI/CD Automation:** Auto-deploy on any cloud, hands-off management, DevOps friendly by design
- **Utmost Efficiency:** No Signiture Update, No False Positives, No Manual Tuning

Cloud Distributed WAF

CloudGuard WAF can be deployed across various platforms including on-premises,agents, gateways, and SaaS. Our team is dedicatedly engaged in regularly enhancing and expanding our support for both widely adopted and cutting-edge technologies.



SUPPORTED ENVIRONMENTS

CLOUD

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure
- VMware

CONTAINERS

- Docker
- Kubernetes
- Kubernetes Ingress

CPU'S

- X86 (64 bit)

OPERATING SYSTEMS

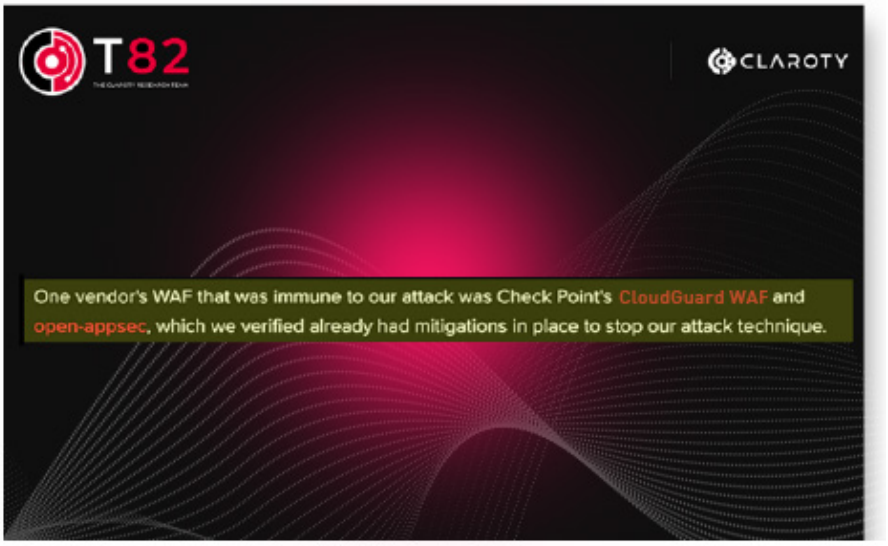
- CentOS
- Debian
- Red Hat Enterprise Linux
- Ubuntu

PROTECTION CATEGORIES

- Cross Site Request Forgery
- XML External Entity
- Remote Code Execution
- Evasion Techniques
- LDAP Injection
- Path Traversal
- Vulnerability Scanning
- SQL Injection
- Illegal HTTP Methods Invalid input to forms and APIs Bot Scraping and Brute Force Attacks
- Over 2800 Web Specific CVEs

Dec 2022 - CloudGuard WAF Recognized as the Only WAF to successfully block a penetration test by Team82

Claroty Team82 has developed a generic bypass for web application firewalls (WAF). Major WAF products including: AWS, F5, CloudFlare, Imperva and Palo Alto were found to be vulnerable. CloudGuardd WAF pre-emptively blocked the attack/bypass, within seconds.



CLOUDGUARD NAMED LEADER IN GIGAOM 2024 RADAR REPORT FOR APPLICATION AND API SECURITY FOR 2 YEARS IN A ROW

"The biggest strength of the CloudGuard WAF solution is API protection. While All Vendors can either import or detect APIs and most vendors can do both, CloudGuard is able to do both and generate sample protection rules based upon the definition and information gleaned from traffic. ***This earned them our highest score on the API import and discovery key feature."***

Don Mcvittie, Analyst | GigaOm

Available for

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com